

(12)特許協力条約に基づいて公開された国際出願

Rec'd PCT/PTO

15 MAR 2005

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 1 月 20 日 (20.01.2005)

PCT

(10) 国際公開番号
WO 2005/006231 A1

- (51) 国際特許分類⁷: G06F 17/60, 15/00, 12/14
- (21) 国際出願番号: PCT/JP2004/008854
- (22) 国際出願日: 2004 年 6 月 17 日 (17.06.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-273315 2003 年 7 月 11 日 (11.07.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電
器産業株式会社 (MATSUSHITA ELECTRIC INDUS-
TRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大
字門真 1 0 0 6 番地 Osaka (JP).

(WAKAMORI, Masahiro). 森田 かおる (MORITA,
Kaoru).(74) 代理人: 岩橋 文雄, 外 (IWAHASHI, Fumio et al.); 〒
5718501 大阪府門真市大字門真 1 0 0 6 番地 松下電
器産業株式会社内 Osaka (JP).(81) 指定国 (表示のない限り、全ての種類の国内保護が
可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,
BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,
ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI,
NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,
SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.

(72) 発明者; および

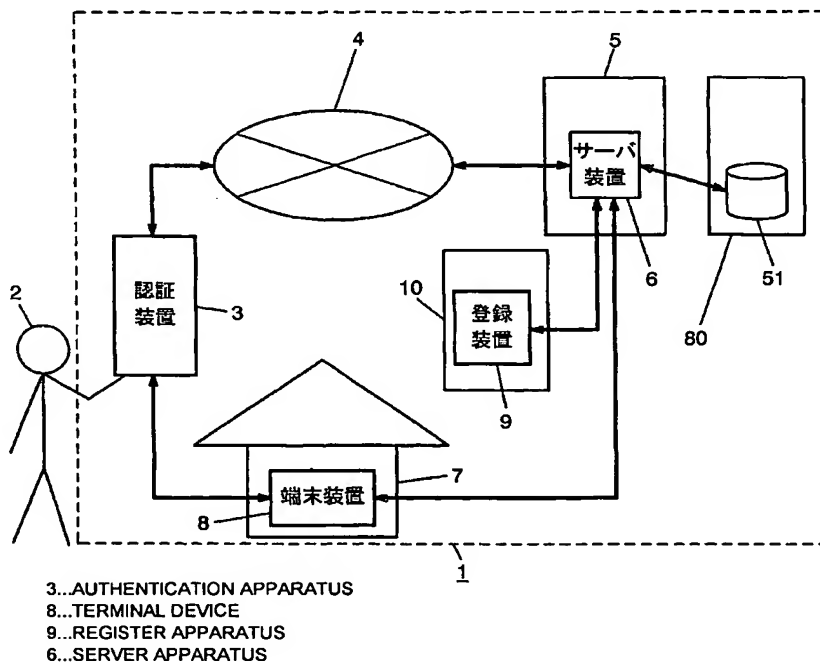
(75) 発明者/出願人 (米国についてのみ): 若森 正浩

(84) 指定国 (表示のない限り、全ての種類の広域保護が可
能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[続葉有]

(54) Title: AUTHENTICATION SYSTEM

(54) 発明の名称: 認証システム



(57) Abstract: An authentication system of a high security property wherein even when a person, who attempts to conduct an illegal behavior, performs modification or the like of an authentication apparatus, a system of a retail store or the like, such an illegal behavior cannot be easily conducted. The authentication system comprises an authentication apparatus that includes an authentication part for authenticating whether a user is a person who has already registered, and also includes an information output part for

[続葉有]



SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

outputting identification information of the user if the user is authenticated as the registered person. The authentication system further comprises a server apparatus that includes an information entering part for entering user identification information, also includes a credibility deciding part for deciding, based on the identification information, the credibility of the user, and further includes a decision result output part for outputting a decision result of the credibility deciding part.

(57) 要約: 不正な行為を行おうとする者が認証装置や小売店のシステム等の改造等を行っても、容易に不正な行為を行うことができないセキュリティ性の高い認証システムであって、ユーザがあらかじめ登録された者であるか否かを認証する認証処理を行う認証処理部と、ユーザがあらかじめ登録された者であると認証された場合にユーザの識別情報を出力する情報出力部とを有する認証装置、ならびに、ユーザの識別情報を入力する情報入力部と、識別情報にもとづいてユーザの信用判定を行う信用判定部と、信用判定部での判定結果を出力する判定結果出力部とを有するサーバ装置を備えた。

明細書

認証システム

5

技術分野

本発明は、画像を用いて本人認証を行う認証装置ならびに認証装置を用いた認証システムに関する。

背景技術

10 近年、人体の個体別に特有の情報（いわゆるバイオメトリクス情報）を認証情報として用いて本人認証を行う認証装置が実用化されており、このような認証装置を用いて、ネットワークを介して物品購買等の情報のやり取りを行うことのできる認証システムが実用化されてきている。

例えば、指紋を認証情報として用いた認証装置と、認証装置と通信が可能な小売店のレジスタとで構成された物品購買の可能な商取引システムに関する技術が
15 特開 2003-6549 号公報に提案されている。

このような技術において、ユーザが小売店の店頭において物品を購入したい場合には、まずユーザは自らが所有する携帯電話装置に搭載された認証装置で認証を行い、本人であることを示す識別情報を携帯電話装置から店頭に配置されたレジスタに送信する。そして小売店では、レジスタからユーザが口座を有する金融機関のサーバ装置に対して、ユーザの識別情報を送るとともに、そのユーザが物品に対する支払い能力を有するか否かの問い合わせを行い、サーバ装置がユーザについてその物品に対する支払い能力があると判定（以下、この判定を信用判定と記す）した場合に取引が成立し、その都度、または契約決済時期に物品の代金
20 がユーザの口座から引き落とされる構成であった。

しかしながら、前述のような商取引システムに関する技術においては、小売店側や認証装置側で、様々な不正な行為が行われる可能性があった。すなわち、その一例として、前述した従来の技術においては、認証装置からレジスタにユーザの識別情報が送信される。また、ユーザの識別情報の送信および信用判定の問い

合わせは、レジスタから金融機関のサーバ装置に対して行われ、ユーザが支払い能力を有するとサーバ装置が判定した場合に、ユーザの口座から物品の対価が小売店側の口座に振り込まれる。従って、例えば小売店側において、レジスタにあらかじめ所定のユーザの識別情報を記憶しておき、あたかもそのユーザが物品を
5 購入するように見せかけて、レジスタからサーバ装置に対して所定のユーザの識別情報および信用判定の問い合わせを行い、支払い能力を有すると判定されることにより、実際には販売していない物品に対する対価を自らの口座に振り込ませるような行為が行われる可能性があるという課題があった。

10 発明の開示

本発明はこのような課題に鑑みてなされたもので、容易に不正な行為を行うことのできない、セキュリティ性の高い認証システムを提供することを目的とする。

このような課題を解決するために、本発明の認証システムは、被認証者があらかじめ登録された者であるか否かを認証する処理を行う認証処理部と、被認証者
15 があらかじめ登録された者であると認証された場合に被認証者の識別情報を出力する情報出力部とを有する認証装置、ならびに、情報出力部が出力した被認証者の識別情報にもとづいて被認証者の信用判定を行う信用判定部と、信用判定部での判定結果を出力する判定結果出力部とを有するサーバ装置を備えたことを特徴としている。

20 このような構成によれば、被認証者の識別情報は、被認証者の認証が行われた後に認証装置からサーバ装置に送られ、サーバ装置において被認証者の信用判定が行われるので、他の装置、例えば小売店側のレジスタやPOS装置（以下、端末装置と記す）を改造等しても、被認証者の識別情報を抜き取ったり、ユーザに成り代わって識別情報および信用判定を要求したりすることができないので、小
25 売店側において容易に不正な行為を行うことができないセキュリティ性の高い認証システムを提供できる。

また、認証装置は画像を入力するための画像入力部を有し、認証処理部は画像入力部が入力した入力画像にもとづいて被認証者の認証を行う構成であってもよい。

このような構成によれば、さらに、被認証者のバイオメトリクス情報、例えば指紋パターン、虹彩パターン、顔の形状パターン、網膜パターン等を用いた認証率の高い認証処理を行うことができる。

- 5 さらに、入力画像が被認証者の眼画像であり、認証処理部は、眼画像から被認証者の虹彩パターンにもとづいた認証情報を作成する認証情報作成部、登録認証情報を記憶する記憶部、および、登録認証情報と眼画像から作成された認証情報とを比較照合する比較照合部を有する構成であってもよい。

このような構成によれば、さらに、本人排除率および他人受入率の低い、より高精度な本人認証を行うことができる。

- 10 次に、本発明の認証システムは、サーバ装置から出力された判定結果を入力する判定結果入力部を有する端末装置を備えたことを特徴としている。

- このような構成によれば、被認証者の識別情報は、被認証者の認証が行われた後に認証装置からサーバ装置に送られ、サーバ装置において被認証者の信用判定が行われ、その結果が端末装置に送られるので、他の装置、例えば小売店側の端
15 末装置を改造等しても、被認証者の識別情報を抜き取ったり、ユーザに成り代わって識別情報および信用判定を要求したりすることができないので、小売店側において容易に不正な行為を行うことができないセキュリティ性の高い認証システムを提供できる。

- また、認証装置は取引すべき物品に関する情報を含む情報を入力する情報入力
20 部を有し、端末装置は、認証装置の情報入力部に対して取引すべき物品に関する情報を含む情報を出力する情報出力部を有する構成であってもよい。

- このような構成によれば、さらに、物品が購入可能であるか否かの情報や取引
対象となる物品等の情報を端末装置から認証装置に対して出力することができ、
被認証者は自ら信用判定の結果や取引対象となる物品等の情報を知ることができ
25 る。

次に、本発明の認証システムは、登録すべき者の登録認証情報および所定の認証処理を行う認証処理部を記憶する記憶部、ならびに、登録認証情報および認証処理部を出力する情報出力部を有するサーバ装置と、被認証者の認証情報を取得する認証情報取得部、登録認証情報および認証処理部を入力する情報入力部、な

らびに、認証情報を用いて所定の演算処理を行う演算処理部を有する認証装置とを備えた認証システムであって、認証装置は、サーバ装置から入力した認証処理部を演算処理部に読み込み、演算処理部に読み込んだ認証処理部によって、被認証者の認証情報と登録認証情報とを比較照合することを特徴としている。

- 5 このような構成によれば、認証装置側にはあらかじめ登録認証情報および認証処理部を搭載しておらず、サーバ装置側から登録認証情報および認証処理部を受信してから認証処理を行うので、被認証者が登録認証情報を偽造して認証装置を使用すべき者になりすますことの難しいセキュリティ性の高い認証システムを実現できる。また、このような構成によれば、サーバ装置側から認証装置に対して
- 10 認証処理部を送信するので、例えば認証処理部がソフトウェアである場合、認証処理部のバージョンアップ等が行われた場合にも、最新の認証処理を行うことが可能である。

- また、登録すべき者の登録認証情報を取得する登録認証情報取得部および登録認証情報を出力する登録認証情報出力部を有する登録装置を備え、サーバ装置は、
- 15 登録認証情報および認証処理部を入力する情報入力部を有し、登録装置は、登録認証情報取得部で取得された登録認証情報を情報出力部からサーバ装置の情報入力部に対して出力し、サーバ装置は、情報入力部が入力した登録認証情報を記憶部に記憶することを特徴とする構成であってもよい。

- このような構成によれば、さらに、被認証者は認証システムの使用を開始する
- 20 際に、登録装置において取得された自らの認証情報を登録認証情報としてサーバ装置に送り、認証装置はサーバ装置から送られた登録認証情報を参照して認証処理を行うので、登録装置を信用度の高い場所、例えば金融機関や通信キャリア会社等に配置することにより、より信頼度の高い登録認証情報を取得することが可能となり、セキュリティ性の高い認証システムを実現できる。

- 25 さらに、サーバ装置は、認証処理部および登録認証情報を所定の方法で暗号化する暗号化部を有し、記憶部に暗号化された認証処理部および登録認証情報を復号化する復号化部を記憶し、情報出力部から復号化部ならびに暗号化された認証処理部および登録認証情報を出力し、認証装置は、情報入力部が入力した認証処理部および登録認証情報を復号化部によって復号化する構成であってもよい。

このような構成によれば、さらに、サーバ装置の記憶部には暗号化された情報が記憶されており、かつ、認証装置とサーバ装置間での情報の送受信は、暗号化された情報によって行われるので、通信経路等で盗まれたりした場合にも、容易に内容が解読できないので、セキュリティ性の高い構成を実現できる。

- 5 次に、本発明の認証システムは、被認証者の登録認証情報を取得する登録認証情報取得部および登録認証情報を出力する登録認証情報出力部を有する登録装置と、被認証者の認証情報を取得する認証情報取得部、所定の情報の入出力を行う情報入出力部、ならびに、認証情報を用いて所定の演算処理を行う演算処理部を有する認証装置と、認証装置から被認証者の識別情報を、登録装置から登録認証
- 10 情報をそれぞれ入力する情報入力部と、登録認証情報および所定の認証処理を行う認証処理部を記憶する記憶部と、識別情報を用いて被認証者の信用判定を行う信用判定部と、信用判定部での判定結果を出力する判定結果出力部を有するサーバ装置と、サーバ装置から出力された判定結果を入力する判定結果入力部を有する端末装置とを備えた認証システムであって、認証装置は、サーバ装置から入力
- 15 した認証処理部を演算処理部に読み込み、認証処理部によって、被認証者の認証情報と登録認証情報とを比較照合し、被認証者があらかじめ登録された者であると認証された場合に被認証者の識別情報をサーバ装置に出力し、サーバ装置は信用判定部において被認証者の信用判定を行い、その判定結果を端末装置に出力することを特徴としている。
- 20 このような構成によれば、被認証者の識別情報は、被認証者の認証が行われた後に認証装置からサーバ装置に送られ、サーバ装置において被認証者の信用判定が行われるので、他の装置、例えば小売店側のレジスタやPOS装置等の端末装置を改造等しても、被認証者の識別情報を抜き取ったり、ユーザに成り代わって識別情報および信用判定を要求したりすることができないので、小売店側において容易に不正な行為を行うことができないセキュリティ性の高い認証システムを提供できる。また、被認証者は認証システムの使用を開始する際に、登録装置において取得された自らの認証情報を登録認証情報としてサーバ装置に送り、情報
- 25 装置はサーバ装置から送られた登録認証情報を参照して認証処理を行うので、登録装置を信頼性の高い場所、例えば金融機関や通信キャリア会社等に配置するこ

とにより、より信頼度の高い登録認証情報を取得することが可能となり、セキュリティ性の高い認証システムを実現できる。

次に、本発明の認証装置は、画像を入力する画像入力部と、画像から認証情報を作成する認証情報作成部、一の認証情報と他の認証情報とを比較照合する比較照合部、および、登録認証情報を含む情報を入力する情報入力部と、画像および情報入力部が入力した情報を用いて所定の演算を行う演算部とを備え、演算部は、情報入力部から認証情報作成部および比較照合部を読み込み、認証情報作成部が画像から画像に対応する認証情報を作成し、比較照合部が登録認証情報と画像に対応する認証情報とを比較照合することを特徴としている。

- 10 このような構成によれば、認証装置側には秘匿すべき登録認証情報、認証情報作成部または比較照合部を搭載しておらず、外部装置から登録認証情報および認証処理部を受信してから認証処理を行うので、被認証者が登録認証情報を偽造して認証装置を使用すべき者になりすますことの難しい、認証装置が壊されたり情報が盗まれたりする等のタンパ行為等を受けた場合にも、重要な情報が外部にも
- 15 れるようなことがなく、セキュリティ性の高い構成を実現できる。また、外部装置から受信した認証処理部を用いて認証処理を行うので、例えば認証情報作成部または比較照合部等の認証処理部がソフトウェアである場合、認証処理部のバージョンアップ等が行われた場合にも、最新の認証処理を行うことが可能である。

- 20 また、登録認証情報が暗号化された情報であり、情報入力部が登録認証情報を復号する復号部を入力し、復号部が復号した登録認証情報と画像に対応する認証情報とを比較照合部が比較照合する構成であってもよい。

- 25 このような構成によれば、さらに、外部装置と認証装置との間での情報の送受信は、暗号化された情報によって行われるので、通信経路等で盗まれたりした場合にも、容易に内容が解読できないので、セキュリティ性の高い構成を実現できる。

また、画像が被認証者の眼画像であり、認証情報作成部は、眼画像から被認証者の虹彩パターンにもとづいた認証情報を作成する構成であってもよい。

このような構成によれば、さらに、本人排除率および他人受入率の低い、より高精度な本人認証を行うことができる。

次に、本発明のサーバ装置は、認証情報を含む情報を入力する情報入力部と、認証情報を暗号化して登録認証情報とする暗号化部と、登録認証情報を記憶した記憶部と、記憶部に記憶された情報の出力を行う情報出力部とを備えたことを特徴としている。

- 5 このような構成によれば、サーバ装置の記憶部には暗号化された情報が記憶されており、かつ、外部装置とサーバ装置間での情報の送受信は、暗号化された情報によって行われるので、セキュリティ性の高い構成を実現できる。

- また、記憶部は、画像から認証情報を作成する認証情報作成部、一の認証情報と他の認証情報とを比較照合する比較照合部、および、登録認証情報を復号化する復号化部を記憶する構成であってもよい。
- 10

このような構成によれば、さらに、認証処理部を有しない他の情報装置に対して、記憶部に記憶された認証情報作成部、比較照合部および復号化部を送信することにより、その情報装置において認証処理を実現させることが可能である。

- 次に、本発明の登録装置は、登録すべき者の画像を入力する画像入力部と、画像から所定の認証情報を作成する認証情報作成部と、登録すべき者の個人情報を
- 15 入力する個人情報入力部と、認証情報および個人情報を出力する情報出力部を備えたことを特徴としている。

- このような構成によれば、被認証者から取得した認証情報および個人情報を外部に出力することができるので、このような登録装置を安全性が高い場所、例えば金融機関や通信キャリア会社等に配置して認証システムを構成することにより、より信頼度の高い登録認証情報を取得することが可能となり、高いセキュリティ性を実現できる。
- 20

また、画像が登録すべき者の眼画像であり、認証情報作成部は、眼画像から登録すべき者の虹彩パターンにもとづいた認証情報を作成する構成であってもよい。

- 25 このような構成によれば、さらに、本人排除率および他人受入率の低い、より高精度な本人認証を行うことができる認証情報を、登録認証情報として登録できる。

次に、本発明の端末装置は、物品の購入を行う者の信用判定の結果を入力する判定結果入力部と、信用判定の結果にもとづいて物品の購入を認めるか否かを示

す情報を含む情報を出力する情報出力部を備えたことを特徴としている。

このような構成によれば、サーバ装置等の他の装置から信用判定の結果を受信してから物品を購入する者に対して物品の購入が可能であるか否かを出力したり、ユーザに対して購入すべき物品の金額等についての情報を送信したりするので、

5 セキュリティ性の高い、ユーザにとって負担の小さい構成を実現できる。

また、情報出力部は、物品の購入を認めるか否かを示す情報を含む情報を、赤外線を用いて出力する構成であってもよい。

このような構成によれば、さらに、例えば登録装置から電話装置と兼用する認証装置に対して赤外線による情報出力を行った場合に、電話回線等を用いないので、低コストでシステム構成を実現できる。

10

以上述べたように、本発明の認証装置、サーバ装置または認証システムを用いれば、不正な行為を行おうとする者が認証装置や小売店のシステム等の改造等を行っても、容易に不正な行為を行うことができないセキュリティ性の高い構成を実現できる。

15

図面の簡単な説明

図1は、本発明の実施の形態における認証システムの概略構成を示すブロック図である。

20

図2は、本発明の実施の形態における認証装置の構成の一例を示すブロック図である。

図3は、本発明の実施の形態における認証装置の外観の一例を示す図である。

図4は、本発明の実施の形態におけるサーバ装置の構成の一例を示すブロック図である。

25

図5は、本発明の実施の形態におけるサーバ装置の登録認証情報テーブルを説明するための図である。

図6は、本発明の実施の形態における登録装置の構成の一例を示すブロック図である。

図7は、本発明の実施の形態における端末装置の構成の一例を示すブロック図である。

図 8 は、本発明の実施の形態における認証システムの利用申請時の動作を説明するための図である。

図 9 は、本発明の実施の形態における認証システムの物品購入時の動作を説明するための図である。

5 図 10 は、本発明の実施の形態における申請画面の一例を示す図である。

図 11 は、本発明の実施の形態における認証開始画面および認証完了画面の一例を示す図である。

図 12 は、本発明の実施の形態における利用許可画面の一例を示す図である。

図 13 は、本発明の実施の形態における商品リスト画面の一例を示す図である。

10 図 14 は、本発明の実施の形態における取引確認画面および取引完了画面の一例を示す図である。

発明を実施するための最良の形態

(実施の形態)

15 以下、本発明の実施の形態として、本発明の認証装置およびサーバ装置ならびに認証システムについて、図面を用いて説明する。

まず、本発明の実施の形態における認証システムの構成について図 1 を用いて説明する。図 1 は、本発明の実施の形態における認証システム 1 の概略構成を示すブロック図である。

20 図 1 に示したように、本発明の実施の形態における認証システム 1 は、ユーザ 2 が電話機能を備えた認証装置 3 を用いて小売店 7 において販売されている物品等を購入できる商取引の可能なシステムである。認証装置 3 と小売店 7 の端末装置 8 との情報の送受信は認証装置 3 の電話回線を提供する通信キャリア会社 5 に備えられたサーバ装置 6 を介して行われる。また、物品等の代金は通信キャリア

25 会社 5 から小売店 7 に対して支払われ、もしくは通信キャリア会社 5 がユーザ 2 のクレジットを決済して、その代金はユーザ 2 が通信キャリア会社 5 への通話料金の支払いのために設けた金融機関 80 の口座から引き落とされる。認証装置 3 とサーバ装置 6 との信号の送受信はネットワーク 4 を介して行われる。

本発明の実施の形態における認証システム 1 の利用を開始するには、ユーザ 2

はあらかじめ通信キャリア会社5またはその営業所10に出向いて、そこに配置された登録装置9において、後述する登録のための手続きをしなければならない。

次に、本発明の実施の形態における認証システム1を構成するそれぞれの装置について詳細に説明する。

5 図2は本発明の実施の形態における認証装置3の構成の一例を示すブロック図である。

図2に示したように、本発明の実施の形態における認証装置3は、ユーザ2の眼を含む画像（以下、眼画像と記す）を入力するための画像入力部33、ネットワーク等を介してサーバ装置6と情報の送受信を行う入出力部36、入出力部3
10 6に入力された情報を記憶する記憶部35、画像入力部33から入力された画像情報、記憶部35に記憶された情報、または入出力部36から入力された情報を用いて後述する所定の認証処理を含む演算を行う演算部34、ならびに、演算部34で演算された結果等の表示を行う表示部37を備えている。

また、本発明の実施の形態における認証装置3の外観は、図3に一例を示した
15 ように携帯電話装置の形態と類似しており、図示しないが、携帯電話装置が通常有する通話、メールの送受信または画像の撮影等の機能を有している構成であってもよい。

図3に示したように、本発明の実施の形態における認証装置3の画像入力部33は、近赤外光（波長が700～1000nm程度の光線をいう）を発する光源
20 38をユーザ2の眼の領域に照射して、その反射光の光学系31を透過した光像を撮影する。ユーザ2は鏡部39に自分の眼を映すことで、眼を光学系31の撮影画角内に誘導することができる。なお、本発明の認証装置の画像入力部33は少なくとも光学系31を有する構成であればよく、液晶ディスプレイ等の表示手段やスピーカ等の音声発生手段等によってユーザ2の眼の位置を誘導する場合には鏡部39を含まない構成であってもよい。また、屋外等十分な明るさを有する
25 場所において使用する場合や、光源部を外部に別途有する構成の場合には、特に画像入力部33に光源38を含まない構成であってもよい。しかしながら、実用性に鑑みて鏡部39や光源38を備えることが望ましい。

表示部37としては携帯電話装置等に広く用いられる液晶やEL（E l e c t

ro-Luminescent)等の表示デバイスを適宜用いることができる。

なお、本発明の実施の形態における認証装置3は電話機能を有する例を示したが、本発明の認証装置は電話機能を有する構成に限定されないことはいうまでもない。画像入力部33を有する装置であれば、小型のパーソナルコンピュータ、

5 PDA(Personal Digital Assistant)、デジタルカメラ等の情報装置を用いることができることはいうまでもない。

このように、本発明の実施の形態における認証装置3は、通常時に画像入力部33によって眼画像を撮影することができる。さらに、以下に述べるように、本発明の実施の形態における認証装置3は、演算部34に所定のソフトウェアを読み込み、実行することにより、認証処理を行うことが可能である。

10

次に、本発明の実施の形態において、認証システム1の使用が可能になった場合の認証装置3の構成について説明する。

なお、ここで、認証装置3において「認証システム1の使用が可能になった場合」とは、認証装置3が、後述する切出部40、コード化部41および判定部42(以下、切出部40、コード化部41および判定部42を認証処理部60と記す)、復号化部43ならびに登録認証情報50を、サーバ装置6から入出力部36を通して受信した状態をいう。

15

図2に示したように、認証システム1の使用が可能になった場合においては、認証装置3は、その演算部34に、画像入力部33から入力された画像を所定の大きさの画像に切出す切出部40、切出部40が切出した画像を所定の方法でコード化するコード化部41、記憶部35が記憶する登録認証情報50を復号化する復号化部43、および、コード化部41がコード化して作成した認証情報と、復号化部43が復号化した登録認証情報50とを比較照合して一致するか否かを判定する判定部42とを備える。

20

ここで、本発明の実施の形態における認証装置3においては、切出部40、コード化部41、判定部42または復号化部43は、それぞれソフトウェアであり、サーバ装置6からこれらのソフトウェアが送信され、認証装置3の入出力部36または記憶部35から演算部34に読み込まれ、演算部34でそれぞれのソフトウェアの機能が実行される。

25

なお、切出部 4 0 における画像の切出し方法、コード化部 4 1 による画像のコード化方法、判定部 4 2 における認証情報同士の比較照合の方法、すなわち認証処理部 6 0 における認証処理の方法としては、例えば特許第 3 3 0 7 9 3 6 号公報に記載された方法を用いることができる。

- 5 なお、登録認証情報 5 0 とは、ユーザ 2 の目の虹彩パターンをコード化した、比較照合されるべき認証情報のことをいうものとする。

- また、記憶部 3 5 に記憶された登録認証情報 5 0 は、サーバ装置 6 において所定の方法で暗号化されているものとし、復号化部 4 3 は、暗号化された登録認証情報 5 0 を復号化する機能を有する。認証情報の暗号化方法としては、例えば、
10 認証情報を構成するビットを一定の方法で並べ替えることにより暗号化する方法を用いることができる。なお、本発明はこの認証情報の暗号化方法または対応する復号化方法を限定するものではないことはいうまでもなく、他の公知の暗号化方法または復号化方法も適宜用いることができる。

- 前述のような認証処理部 6 0、復号化部 4 3 によって復号化した登録認証情報
15 5 0 を演算部 3 4 に読み込んで実行することにより、認証装置 3 は、ユーザ 2 の眼画像を撮影し、その虹彩パターンをコード化した認証情報と復号化された登録認証情報 5 0 とを比較照合することによってそのユーザ 2 の本人認証を行うことができる。

- 次に、本発明の実施の形態におけるサーバ装置 6 の構成について説明する。図
20 4 は、本発明の実施の形態におけるサーバ装置 6 の構成の一例を示すブロック図である。本発明の実施の形態においては、サーバ装置 6 はユーザ 2 が加入している通信キャリア会社 5 に備えられているものとして説明する。なお、本発明のサーバ装置はその配置されるべき場所を限定するものではなく、他のクレジット会社や金融機関等に配置される構成であってもよいことはいうまでもない。

- 25 図 4 において、本発明の実施の形態におけるサーバ装置 6 は、認証装置 3 や登録装置 9 または端末装置 8 との信号の入出力を行う入出力部 6 6、入出力部 6 6 が入力した認証情報を、前述の方法で暗号化して登録認証情報 5 0 を作成する暗号化部 6 4、認証システム 1 を利用している全ユーザの登録認証情報 5 0 を含む後述する登録認証情報テーブル 7 0、前述の切出部 4 0、コード化部 4 1 または

判定部 4 2 からなる認証処理部 6 0 および復号化部 4 3 を記憶するデータベース部 6 2、ならびに、入出力部 6 6 を通して入力される情報にもとづいてデータベース部 6 2 へのデータの読み書きを制御したり、ユーザ 2 の信用判定をしたりする制御部 6 1 を備えている。また、制御部 6 1 は、上述の機能以外に、さらに後述する課金情報を金融機関 8 0 のサーバ 5 1 に送信する機能をも有する構成であってもよい。

ここで、登録認証情報テーブル 7 0 について説明する。図 5 に登録認証情報テーブル 7 0 の一例を示す。登録認証情報テーブル 7 0 は、認証システム 1 を利用するユーザ毎に、その ID 番号（識別番号）、氏名、住所、電話番号、認証システム利用許可の有無、認証システム利用の有効期限、登録認証情報または信用情報（あらかじめ定められた金額の支払いが可能であるか否か）等の情報を格納している。これにより、本発明の実施の形態におけるサーバ装置 6 は、購入希望者が認証装置 3 から物品購入の意思を示す情報を入力した場合には、その者を識別すると共に、信用判定を行うことが可能となる。

このような構成により、本発明の実施の形態のサーバ装置 6 は、認証システム 1 を利用することができる全ユーザについての登録認証情報 5 0 を記憶すると共に、データベース部 6 2 に記憶された認証処理部 6 0 を、入出力部 6 6 を通して認証装置 3 に送信することが可能である。サーバ装置 6 のデータベース部 6 2 には、認証情報を前述の方法で暗号化した登録認証情報 5 0 が記憶されているので、もし不正な行為を行おうとする者がデータベース部 6 2 に格納された登録認証情報 5 0 を複製したり、盗んだりしたような場合でも、登録認証情報 5 0 は暗号化されているので、登録認証情報 5 0 をそのまま用いてなりすまし等の不正な行為が行われる可能性をいちじるしく低減させ、セキュリティ性の高いサーバ装置 6 を実現することができる。

なお、本発明の実施の形態におけるサーバ装置 6 の暗号化部 6 4 における暗号化方法は、前述の登録認証情報 5 0 の暗号化方法として説明した方法を用いればよい。

次に、本発明の実施の形態における登録装置 9 の構成について説明する。図 6 は、本発明の実施の形態における登録装置 9 の構成の一例を示すブロック図であ

る。前述のように本発明の実施の形態における登録装置 9 は通信キャリア会社 5 の営業所 10 に配置されているとして説明する。なお、本発明の登録装置は、その配置されるべき場所を限定するものではなく、壊されたり情報が盗まれたりする等のタンパ（いたずら）行為の発生しにくい場所であれば、配置することが可能である。

本発明の実施の形態における登録装置 9 は、サーバ装置 6 との情報を入出力する入出力部 9 6、前述の認証装置 3 の画像入力部 3 3 と同様の機能を有する画像入力部 9 3、前述の認証装置 3 の認証処理部 6 0 のうち切出部 4 0 およびコード化部 4 1 と同様の機能を有する認証情報作成部 9 1、認証システム 1 の使用を開始する旨の情報や、ユーザ 2 の ID、名前、顔写真またはサイン等の個人情報等の情報が入力される情報入力部 9 7、情報入力部 9 7 からの入力にもとづいて認証情報作成部 9 1 から出力される認証情報や個人情報等をサーバ装置 6 に送信する制御部 9 4 を備える。また、ユーザ 2 に個人情報の入力を促す、後述する申請画面を表示する表示部 9 5 を有する構成であってもよい。

本発明の実施の形態においては、登録装置 9 からサーバ装置 6 に認証情報が直接送信される例を示した。これにより、通信キャリア会社 5 と営業所 10 との間の通信の際のデータ量を小さくすることができる。例えば前述の認証情報の例ではそのデータ量を 512 バイトとすることができる。なお、一般に通信キャリア会社 5 とその営業所 10 との間は専用線等、セキュリティ性の高い通信回線が配置されているため、このような構成としたが、インターネット等の一般通信回線を用いる場合には、あらかじめサーバ装置 6 と登録装置 9 との間で所定の暗号化を行った情報の送受信を行うことが望ましいことはいうまでもない。本発明の実施の形態の登録装置 9 においては、情報入力部 9 7 に入力される個人情報にユーザ 2 の顔写真やサインを含めたことにより、信頼度の高い営業所 10 においてユーザ 2 自らが取得した顔写真やサインと認証情報とを合わせてサーバ装置 6 に送って登録することができるので、認証システム 1 の運用の際になりすまし等の不正な行為による問題の発生のおそれをいちじるしく低減させ、信頼性の高いものとすることができる。

次に、本発明の実施の形態における端末装置 8 の構成について図 7 を用いて説

明する。前述のように本発明の実施の形態における端末装置 8 は、ユーザ 2 が購入したい物品を販売する小売店 7 に配置されているとして説明する。

本発明の実施の形態における端末装置 8 は、サーバ装置 6 との間で情報を送受信する入出力部 8 6、ユーザ 2 が購入を希望する物品等の価格や品番等の情報を
5 入力する情報入力部 8 7、所定の情報を表示する表示部 8 3、情報入力部 8 7 に入力された情報を入出力部 8 6 から出力させたり、入出力部 8 6 から入力された情報を表示部 8 3 に表示させたりする制御部 8 4、および、認証装置 3 に対して物品購入が可能か否かを示す情報を出力する情報出力部 8 8 を備える。

情報出力部 8 8 としては、例えば、認証装置 3 に対して電話回線を介して情報
10 を送る構成であってもよいが、コスト面に鑑みて、近年の携帯電話、PDA、パソコン等の情報装置に比較的多く搭載されている IrDA を含む赤外線通信等の、直接通信が可能な方法を用いて情報を送る構成とすることが望ましい。

また、端末装置 8 は図示しない記憶部を有し、その記憶部には、認証システム
1 において端末装置 8 の設置された小売店 7 に対してあらかじめ割当られた ID
15 番号等の識別情報を記憶する構成であってもよい。

次に、本発明の実施の形態における認証システム 1 の動作の一例について、図 8 または図 9 を用いて詳細に説明する。

本発明の実施の形態における認証システム 1 においては、前述のように、ユーザ 2 は認証システム 1 の利用を開始する際に、通信キャリア会社 5 の営業所 1 0
20 に出向いて登録装置 9 において利用申請する。図 8 は、本発明の実施の形態における認証システム 1 の利用申請時の動作を説明するための図である。

図 8 に示したように、ユーザ 2 は登録装置 9 の備え付けられた通信キャリア会社 5 の営業所 1 0 等に出向いて、登録装置 9 に所定の登録を行う。具体的には、登録装置 9 の情報入力部 9 7 から自らの名前、住所等、顔写真またはサイン等の
25 個人情報を入力すると共に、画像入力部 9 3 で眼画像を撮影する。この際、図 1 0 に示したような申請画面 1 1 が、登録装置 9 の表示部 9 5 に表示される構成であれば、よりユーザ 2 が入力を行いやすいので望ましい。登録装置 9 は、画像入力部 9 3 が入力した眼画像を認証情報作成部 9 1 が前述の認証情報の作成を行って、ユーザ 2 に対応した認証情報を作成する。さらに、制御部 9 4 は、個人情報

および認証情報を、入出力部 9 6 を介して通信キャリア会社 5 のサーバ装置 6 に送る (S 1)。

次に、通信キャリア会社 5 のサーバ装置 6 においては、制御部 6 1 が、入出力部 6 6 が入力した情報にもとづいて、ユーザ 2 に対応する ID 番号を付与すると共に、入力した認証情報を暗号化部 6 4 で暗号化して登録認証情報 5 0 を作成する。登録認証情報 5 0 は ID 番号や個人情報と対応付けられてデータベース部 6 2 の登録認証情報テーブル 7 0 に記憶されると共に、登録認証情報 5 0、認証処理部 6 0、および復号化部 4 3 (以下、ID 発行情報と記す) をユーザ 2 に対応した認証装置 3 へ送信する (S 2)。この送信の方法としては、通常の電子メールに ID 発行情報を添付する方法でもよいし、直接 ID 発行情報を認証装置 3 に送る構成であってもよい。認証装置 3 は ID 発行情報を受信すると、図 2 に示したような、認証システム 1 が利用可能な構成となる。

次に、ユーザ 2 は実際に認証システム 1 の利用を開始するために、認証装置 3 がサーバ装置 6 からの ID 発行情報を受信した後に、ユーザ 2 の眼画像を撮影し、認証装置 3 で認証を行う (S 3)。この際、認証装置 3 の表示部 3 7 に、図 1 1 (a) に示したような認証開始画面 1 2 を表示する構成であってもよい。ユーザ 2 は認証装置 3 の画像入力部 3 3 で眼画像を入力し、眼画像は切出部 4 0 で所定の大きさに切出され、コード化部 4 1 でコード化されて、判定部 4 2 へ送られる。また、判定部 4 2 は、記憶部 3 5 に記憶された登録認証情報 5 0 を復号化部 4 3 で復号化した認証情報と、コード化部 4 1 から出力された認証情報とを比較照合して、その結果を入出力部 3 6 に出力する。

ユーザ 2 が認証装置 3 において、認証に成功した場合、すなわち判定部 4 2 からの出力が、ユーザ 2 の本人認証に成功したことを示す信号である場合、その結果が認証装置 3 の入出力部 3 6 からサーバ装置 6 に送られる。この際、認証装置 3 の表示部 3 7 に、図 1 1 (b) に示したような認証完了画面 1 3 を表示する構成であってもよい。

サーバ装置 6 においては、制御部 6 1 が認証装置 3 から送られてきた情報を入出力部 6 6 を通じて受信し、受信した情報が、認証処理が完了して正しく本人認証されたことを示す信号であれば、データベース部 6 2 の登録認証情報テーブル

70 ユーザ2に対応する領域に、認証システム1の利用が可能となった旨の情報を書き込む(S4)。

また、サーバ装置6は、認証装置3に認証システム1の使用が可能となったことを知らせて表示部37はその旨を表示する。この場合、認証装置3の表示部37に、図12に示したような利用許可画面14が表示される構成とすれば、ユーザ2自らが認証システム1を利用可能になったことを確実に理解でき望ましい。図12に示した利用許可画面14においては、ユーザ2のID番号、名前、利用限度額、有効期限、顔写真等の情報が表示されている例を示した。

上述したような動作フローにより、ユーザ2は認証システム1を利用することが可能となる(S5)。

次に、本発明の実施の形態における認証システム1において、ユーザ2が小売店7の物品購入を行う際の動作について説明する。図9は本発明の実施の形態における認証システム1において、ユーザ2が物品の購入を行う際の動作を説明する図である。

図9において、ユーザ2が小売店7において、店員等に対して、所定の物品を購入したい旨の意思表示を行う(S11)。なお、ユーザ2が小売店7に対して所定の物品を購入したい旨の情報をネットワーク等を経由して送信してもよいことはいうまでもない。その場合には、ユーザ2は小売店7まで出向く必要がなく、ネットワーク上の仮想店舗等でも物品等の購入を行うことができる。このような場合には、図13に示したような、商品リスト画面15を表示して、ユーザ2に所望の物品等を選択させることが可能である。

小売店7では店員等が端末装置8を操作し、または自動的に、その情報入力部87から該当する物品等の金額や小売店7の店舗ID等の情報をユーザ2の認証装置3宛に送信する(S12)。この送信については、情報をメールに添付して送信する方法であってもよいし、情報を直接送信する方法であってもよい。また、端末装置8から認証装置3へ赤外線通信等を用いて直接情報が送信されてもよいし、通信キャリア会社5のサーバ装置6や他の装置等を経由してもよい。さらに、ユーザ2が、認証装置3の画像入力部33を用いて、店頭に配置された、または、広告等に印刷された、購入したい物品等に対応するバーコード情報を読み込む等

する構成であってもよい。この場合のバーコード情報には、小売店 7 の店舗 ID や購入したい物品等の金額が格納されているものとすればよい。

ステップ S 1 2 において、端末装置 8 から送信された情報にもとづいて、認証装置 3 の表示部 3 7 には、物品の購入意思を確認するためのメッセージが表示される。一例として、図 1 4 (a) に示したような、取引確認画面 1 6 を表示する構成であってもよい。取引確認画面 1 6 においては、購入したい物品名や金額等の情報が表示されていればよい。ユーザ 2 は、認証装置 3 において、自らの眼画像を撮影して本人認証を行う (S 1 3)。この本人認証における認証処理については、前述の通りである。また、認証を行う際には、前述の認証開始画面 1 2 および認証完了画面 1 3 を表示部 3 7 に表示させる構成としてもよい。

認証装置 3 において、ユーザ 2 が正しく本人認証されたとの出力が判定部 4 2 からあった場合、認証が成功したユーザ 2 に対応する個人 ID、店舗 ID または購入すべき物品の金額等の情報 (以下、物品購入情報と記す) が認証装置 3 の入出力部 3 6 から通信キャリア会社 5 のサーバ装置 6 へと送信される。なお、この送信についても、物品購入情報をメールに添付する方法や、物品購入情報を直接送信する方法等公知の方法を適宜選択することが可能である。

サーバ装置 6 の制御部 6 1 では、認証装置 3 から受信した物品購入情報から、ユーザ 2 が所望の物品を購入できるだけの信用を有するか否かの信用判定を行う (S 1 4)。この信用判定は、登録認証情報テーブル 7 0 に格納されたユーザ 2 の過去の通話料等の支払い履歴情報 (以下、信用情報と記す) を参酌してもよいし、あらかじめ所定の上限金額等を定めておき、その上限を超えるか否かによって定めてもよい。信用判定された結果はサーバ装置 6 の制御部 6 1 から端末装置 8 へと送信される。

端末装置 8 は、信用判定された結果を受信して、その結果を確認し (S 1 5)、ユーザ 2 が信用を有すると判定されれば、小売店 7 の店員等からユーザ 2 に対して所望の物品が引き渡されてまたは郵送等されて、ユーザ 2 は所望の物品を受け取ることができる (S 1 6)。ステップ S 1 5 において、ユーザ 2 が物品を購入するに値する信用を有しないと判定された場合には、その情報が端末装置 8 の表示部 8 3 に表示される等して、店員等はその旨をユーザ 2 に告げる、または送信

する等して告知し、取引は成立しない。

5 なお、ステップS 1 4において、サーバ装置6における信用判定結果は、前述のように小売店7の端末装置8へ送られると共に、ユーザ2の認証装置3へも送られ、図1 4 (b) に示したような取引完了画面1 7が表示部3 7に表示されて、
10 ただちにまたは支払い契約日に引き落としがなされる旨の告知がされる(S 1 7)。サーバ装置6からは金融機関8 0のサーバ5 1に対して、引き落としを行う旨の請求が送られる。これによって、ユーザ2は、自らの購入したい物品等についての対価が金融機関8 0の口座から引き落とされることを知ることができる。なお、この対価は、通信キャリア会社5の通話料と合わせて後ほどユーザ2に請求される構成であってもよいことはいうまでもない。

15 このように、本発明の認証装置、サーバ装置または認証システムを用いれば、ユーザ2は認証システム1の利用を開始する際に眼画像の撮影や認証情報の作成を通信キャリア会社5の営業所1 0の登録装置9で行う。一般に通信キャリア会社の営業所のセキュリティ性は高いので、不正な行為を行おうとする者によるなりすましや、認証情報の偽造等が行われる可能性を低くすることができる。

20 また、本発明の認証装置、サーバ装置または認証システムを用いれば、認証システム1を利用開始することが決定されてはじめて認証装置3に認証処理部6 0が送信されるので、システムに対する認証装置3からの不正な行為の発生をいちじるしく低減させることができる。

25 さらに、本発明の認証装置、サーバ装置または認証システムを用いれば、認証装置3とサーバ装置6との認証情報の送受信は、認証情報を暗号化した登録認証情報5 0によって行われるので、装置間で情報が盗まれたり、複製されたりしても、認証情報として用いることのできないセキュリティ性の高い構成を実現できる。

30 さらに、本発明の認証装置、サーバ装置または認証システムを用いれば、ユーザ2が認証システム1を利用開始してはじめて、すなわち、あらかじめ認証された信頼性の高いユーザに対してのみ登録認証情報5 0を復号化する復号化部4 3がサーバ装置6から認証装置3へ送信されるので、セキュリティ性の高い構成を実現できる。

また、本発明の認証装置、サーバ装置または認証システムを用いれば、物品購入情報、すなわち金銭の支払い要求は認証装置 3 からサーバ装置 6 へ送られるので、小売店 7 で架空のユーザ 2 が物品を購入するような物品購入情報を偽造することができない、セキュリティ性の高い構成を実現できる。

- 5 なお、本発明の実施の形態においては、認証情報として、眼画像をコード化することによって得た虹彩にもとづく情報を用いた構成について説明したが、本発明の認証装置、サーバ装置または認証システムにおいては、認証情報は虹彩にもとづいた情報に限定されない。例えば、指紋、眼底の血管パターン、顔等の公知の生体のバイオメトリクス情報を認証情報として用いることが可能である。

10

産業上の利用可能性

- 本発明に係る認証システムならびに認証装置、サーバ装置、登録装置および端末装置は、不正な行為を行おうとする者が認証装置や小売店のシステム等の改造等を行っても、容易に不正な行為を行うことができないセキュリティ性の高い構成
- 15 成を実現できるという効果を有し、画像を用いて本人認証を行う認証装置ならびに認証装置を用いた認証システム等として利用可能である。

請求の範囲

1. 被認証者があらかじめ登録された者であるか否かを認証する処理を行う認証処理部と、前記被認証者があらかじめ登録された者であると認証された場合に前記被認証者の識別情報を出力する情報出力部とを有する認証装置、ならびに、
5 前記情報出力部が出力した前記被認証者の識別情報にもとづいて前記被認証者の信用判定を行う信用判定部と、前記信用判定部での判定結果を出力する判定結果出力部とを有するサーバ装置を備えたことを特徴とする認証システム。
- 10 2. 前記認証装置は画像を入力するための画像入力部を有し、
前記認証処理部は前記画像入力部が入力した入力画像にもとづいて前記被認証者の認証を行うことを特徴とする請求項 1 に記載の認証システム。
- 15 3. 前記入力画像が前記被認証者の眼画像であり、
前記認証処理部は、前記眼画像から前記被認証者の虹彩パターンにもとづいた認証情報を作成する認証情報作成部、登録認証情報を記憶する記憶部、および、前記登録認証情報と前記眼画像から作成された前記認証情報とを比較照合する比較照合部を有することを特徴とする請求項 2 に記載の認証システム。
- 20 4. 前記サーバ装置から出力された前記判定結果を入力する判定結果入力部を有する端末装置を備えたことを特徴とする請求項 1 に記載の認証システム。
- 25 5. 前記認証装置は取引すべき物品に関する情報を含む情報を入力する情報入力部を有し、前記端末装置は、前記認証装置の前記情報入力部に対して前記取引すべき物品に関する情報を含む情報を出力する情報出力部を有することを特徴とする請求項 4 に記載の認証システム。
6. 登録すべき者の登録認証情報および所定の認証処理を行う認証処理部を記憶する記憶部、ならびに、前記登録認証情報および前記認証処理部を出力する情報

出力部を有するサーバ装置と、

被認証者の認証情報を取得する認証情報取得部、前記登録認証情報および前記認証処理部を入力する情報入力部、ならびに、前記認証情報を用いて所定の演算処理を行う演算処理部を有する認証装置とを備えた認証システムであって、

- 5 前記認証装置は、前記サーバ装置から入力した前記認証処理部を前記演算処理部に読み込み、前記演算処理部に読み込んだ前記認証処理部によって、前記被認証者の前記認証情報と前記登録認証情報とを比較照合することを特徴とする認証システム。

- 10 7. 前記登録すべき者の登録認証情報を取得する登録認証情報取得部および前記登録認証情報を出力する登録認証情報出力部を有する登録装置を備え、

前記サーバ装置は、前記登録認証情報および前記認証処理部を入力する情報入力部を有し、

- 15 前記登録装置は、前記登録認証情報取得部で取得された登録認証情報を前記情報出力部から前記サーバ装置の前記情報入力部に対して出力し、前記サーバ装置は、前記情報入力部が入力した前記登録認証情報を前記記憶部に記憶することを特徴とする請求項6に記載の認証システム。

- 20 8. 前記サーバ装置は、前記認証処理部および前記登録認証情報を所定の方法で暗号化する暗号化部を有し、前記記憶部に暗号化された前記認証処理部および前記登録認証情報を復号化する復号化部を記憶し、前記情報出力部から前記復号化部ならびに暗号化された前記認証処理部および前記登録認証情報を出力し、

- 25 前記認証装置は、前記情報入力部が入力した前記認証処理部および前記登録認証情報を前記復号化部によって復号化することを特徴とする請求項6または請求項7に記載の認証システム。

9. 被認証者の登録認証情報を取得する登録認証情報取得部および前記登録認証情報を出力する登録認証情報出力部を有する登録装置と、

前記被認証者の認証情報を取得する認証情報取得部、所定の情報の入出力を行

う情報入出力部、ならびに、前記認証情報を用いて所定の演算処理を行う演算処理部を有する認証装置と、

- 前記認証装置から前記被認証者の識別情報を、前記登録装置から前記登録認証情報をそれぞれ入力する情報入力部と、前記登録認証情報および所定の認証処理を行う認証処理部を記憶する記憶部と、前記識別情報を用いて前記被認証者の信用判定を行う信用判定部と、前記信用判定部での判定結果を出力する判定結果出力部を有するサーバ装置と、
- 5

前記サーバ装置から出力された前記判定結果を入力する判定結果入力部を有する端末装置とを備えた認証システムであって、

- 10 前記認証装置は、前記サーバ装置から入力した前記認証処理部を前記演算処理部に読み込み、前記認証処理部によって、前記被認証者の認証情報と前記登録認証情報とを比較照合し、前記被認証者があらかじめ登録された者であると認証された場合に前記被認証者の識別情報を前記サーバ装置に出力し、前記サーバ装置は前記信用判定部において前記被認証者の信用判定を行い、その判定結果を前記
- 15 端末装置に出力することを特徴とする認証システム。

10. 画像を入力する画像入力部と、

- 前記画像から認証情報を作成する認証情報作成部、一の認証情報と他の認証情報とを比較照合する比較照合部、および、登録認証情報を含む情報を入力する情報入力部と、
- 20

前記画像および前記情報入力部が入力した情報を用いて所定の演算を行う演算部とを備え、

- 前記演算部は、前記情報入力部から前記認証情報作成部および前記比較照合部を読み込み、前記認証情報作成部が前記画像から前記画像に対応する認証情報を作成し、前記比較照合部が前記登録認証情報と前記画像に対応する認証情報とを比較照合することを特徴とする認証装置。
- 25

11. 前記登録認証情報が暗号化された情報であり、

前記情報入力部が前記登録認証情報を復号する復号部を入力し、前記復号部が

復号した前記登録認証情報と前記画像に対応する認証情報とを前記比較照合部が比較照合することを特徴とする請求項 10 に記載の認証装置。

12. 前記画像が被認証者の眼画像であり、

- 5 前記認証情報作成部は、前記眼画像から前記被認証者の虹彩パターンにもとづいた認証情報を作成することを特徴とする請求項 10 または請求項 11 に記載の認証装置。

13. 認証情報を含む情報を入力する情報入力部と、

- 10 前記認証情報を暗号化して登録認証情報とする暗号化部と、
前記登録認証情報を記憶した記憶部と、
前記記憶部に記憶された情報の出力を行う情報出力部とを備えたことを特徴とするサーバ装置。

- 15 14. 前記記憶部は、画像から認証情報を作成する認証情報作成部、一の認証情報と他の認証情報とを比較照合する比較照合部、および、前記登録認証情報を復号化する復号化部を記憶することを特徴とする請求項 13 に記載のサーバ装置。

15. 登録すべき者の画像を入力する画像入力部と、

- 20 前記画像から所定の認証情報を作成する認証情報作成部と、
前記登録すべき者の個人情報を入力する個人情報入力部と、
前記認証情報および前記個人情報を出力する情報出力部を備えたことを特徴とする登録装置。

- 25 16. 前記画像が前記登録すべき者の眼画像であり、

前記認証情報作成部は、前記眼画像から前記登録すべき者の虹彩パターンにもとづいた認証情報を作成することを特徴とする請求項 15 に記載の登録装置。

17. 物品の購入を行う者の信用判定の結果を入力する判定結果入力部と、前記

信用判定の結果にもとづいて前記物品の購入を認めるか否かを示す情報を含む情報を出力する情報出力部を備えたことを特徴とする端末装置。

18. 前記情報出力部は、前記物品の購入を認めるか否かを示す情報を含む情報を、赤外線を用いて出力することを特徴とする請求項17に記載の端末装置。
- 5

FIG. 1

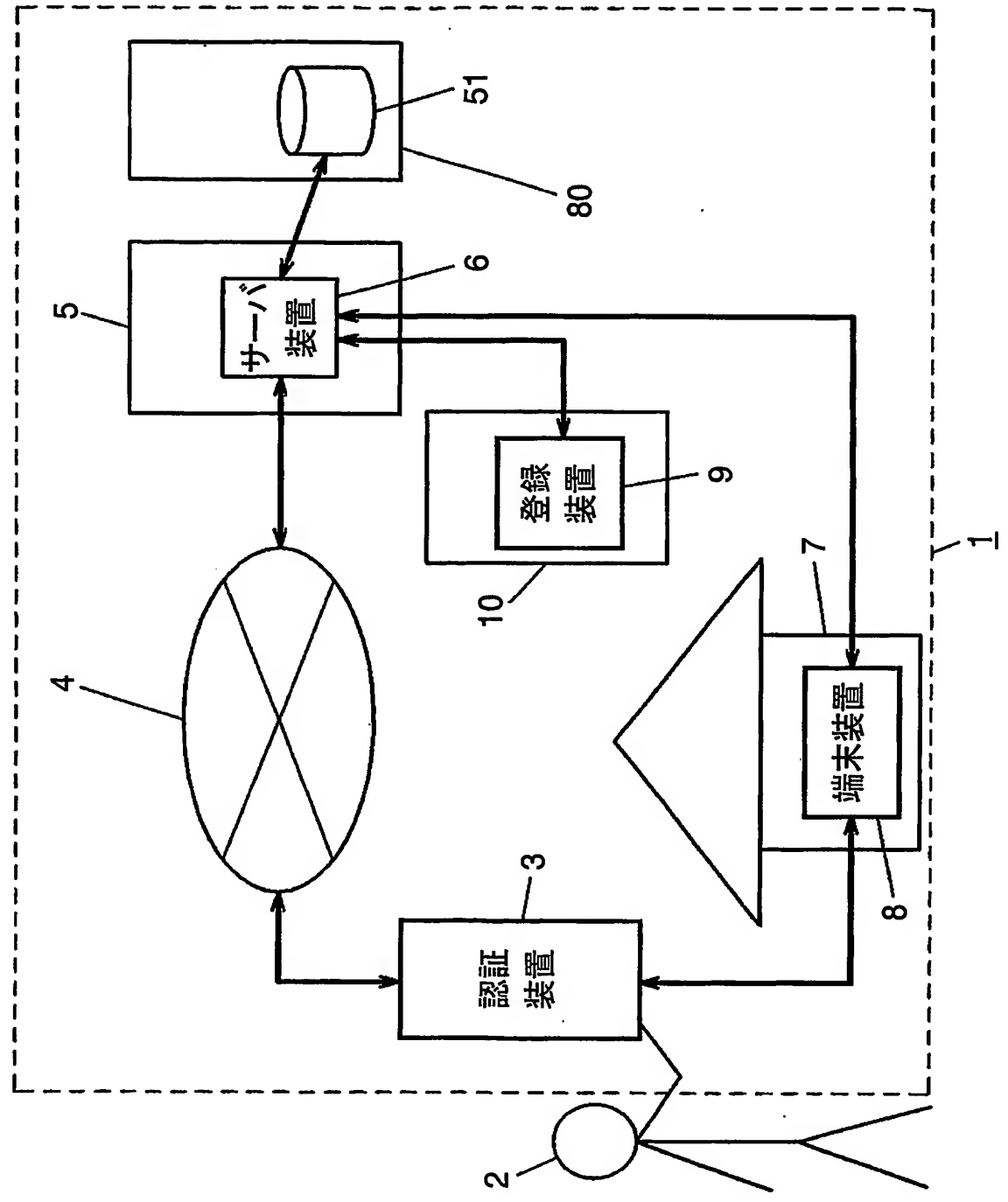
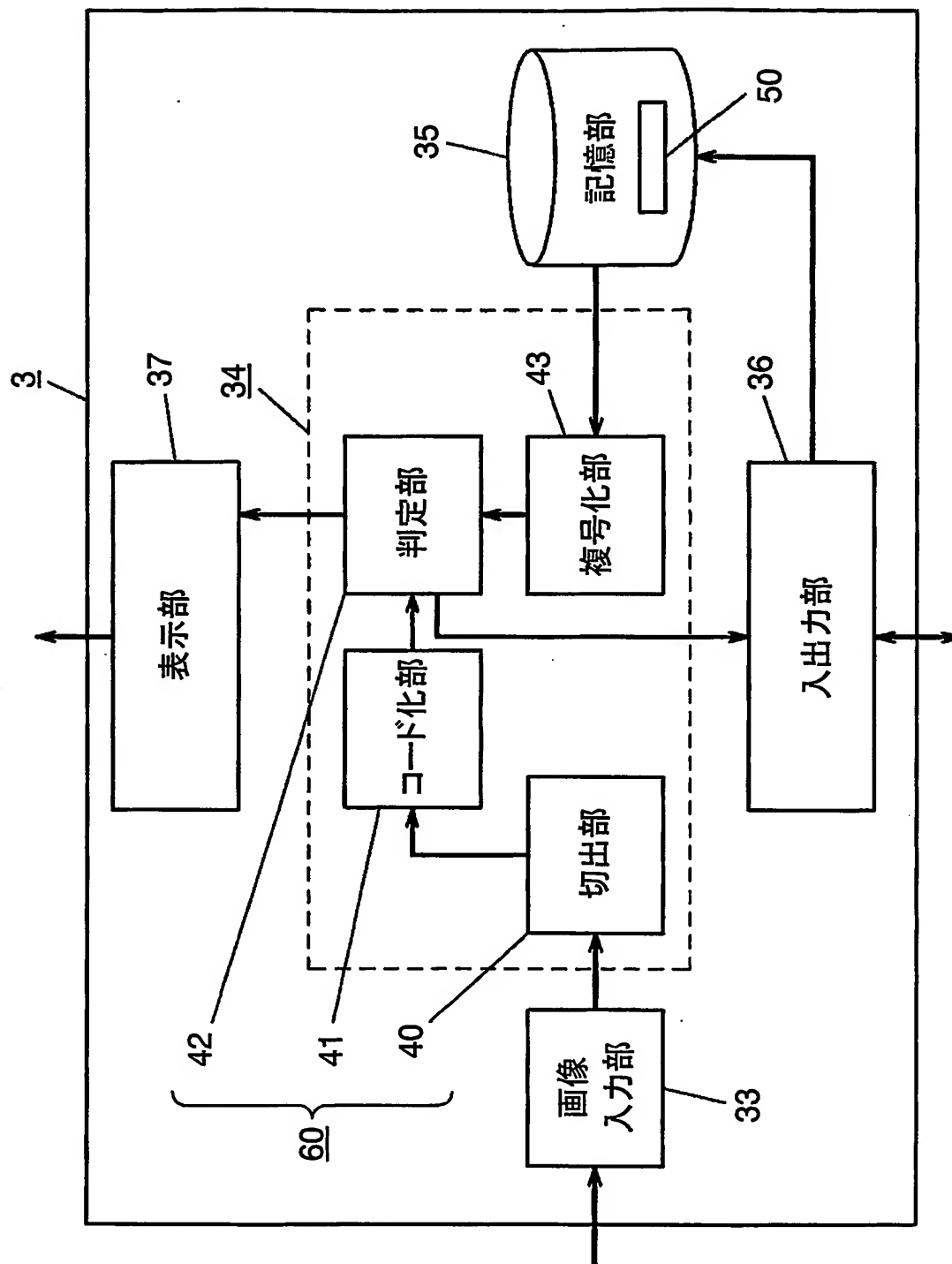
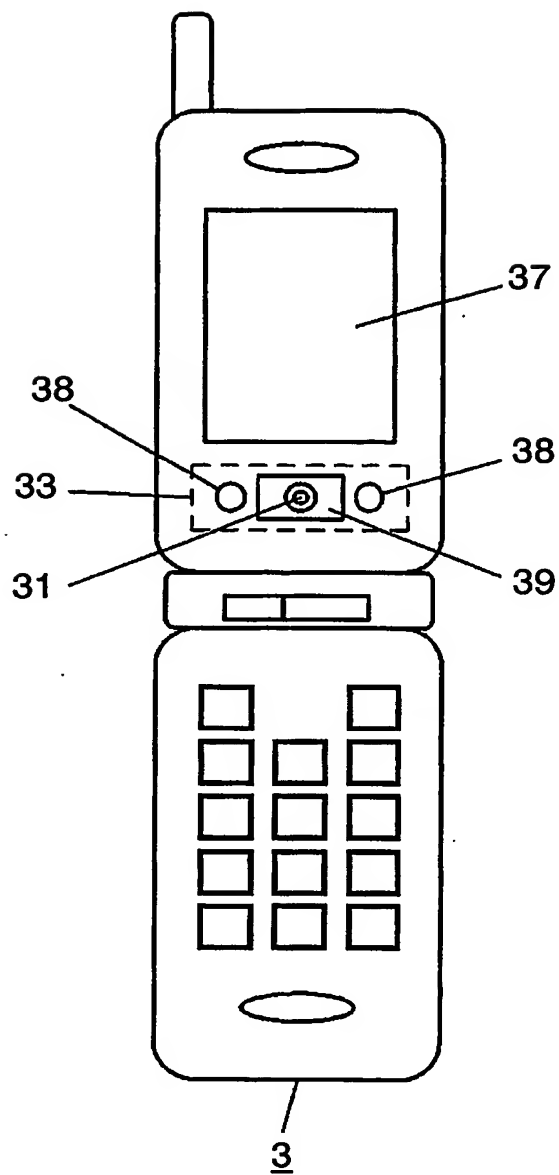


FIG. 2



3/15

FIG. 3



4/15

FIG. 4

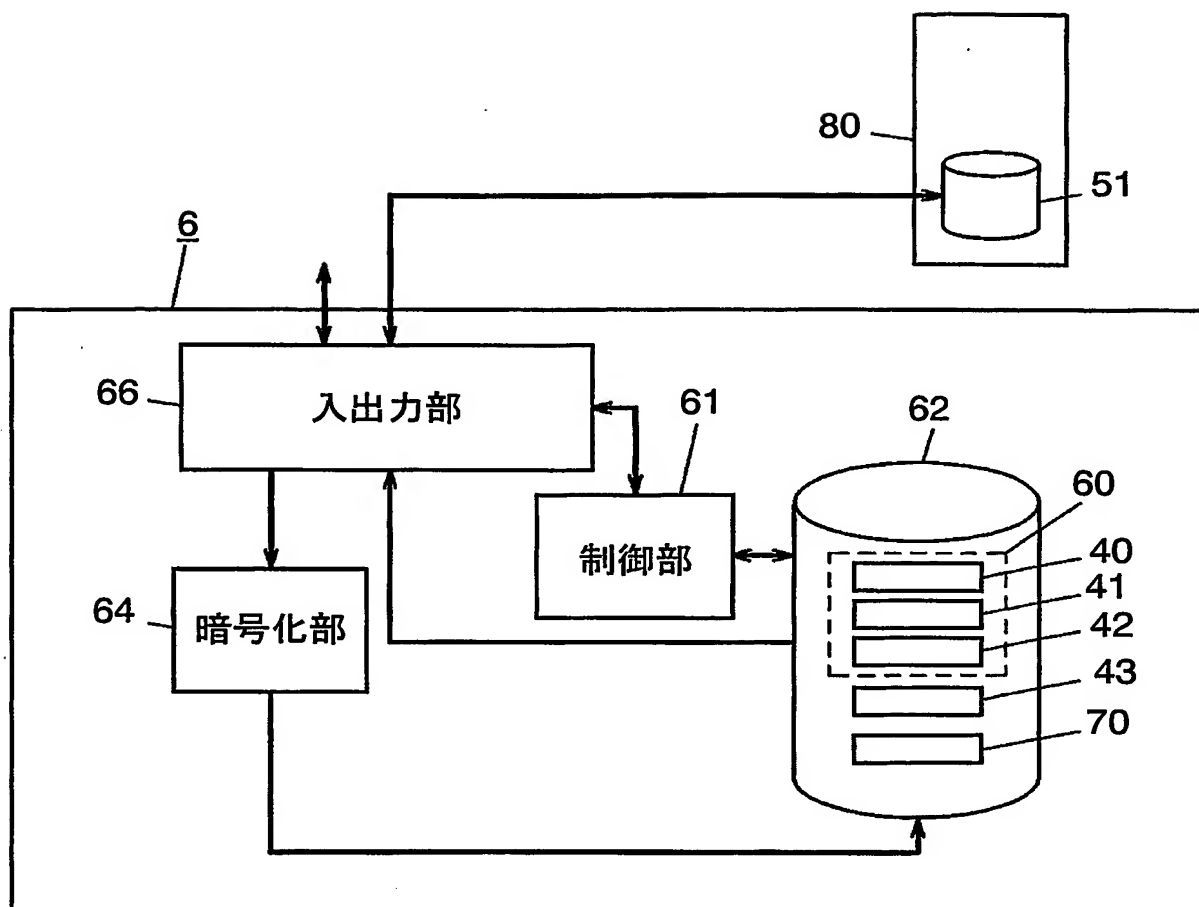


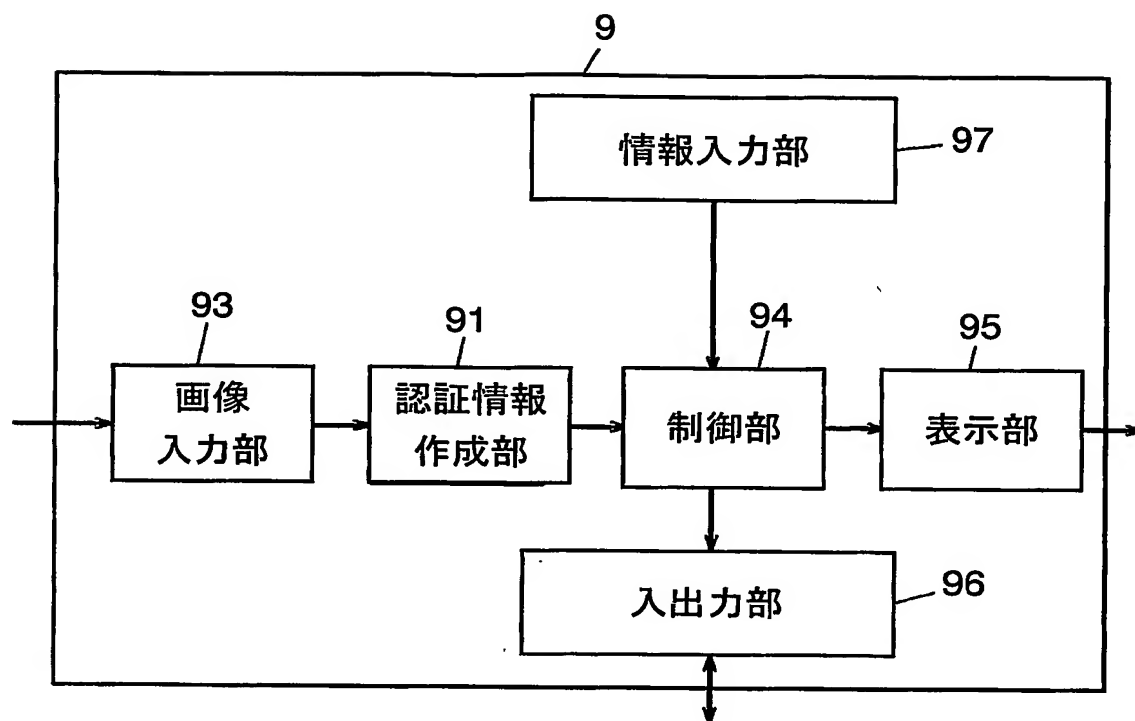
FIG. 5

70

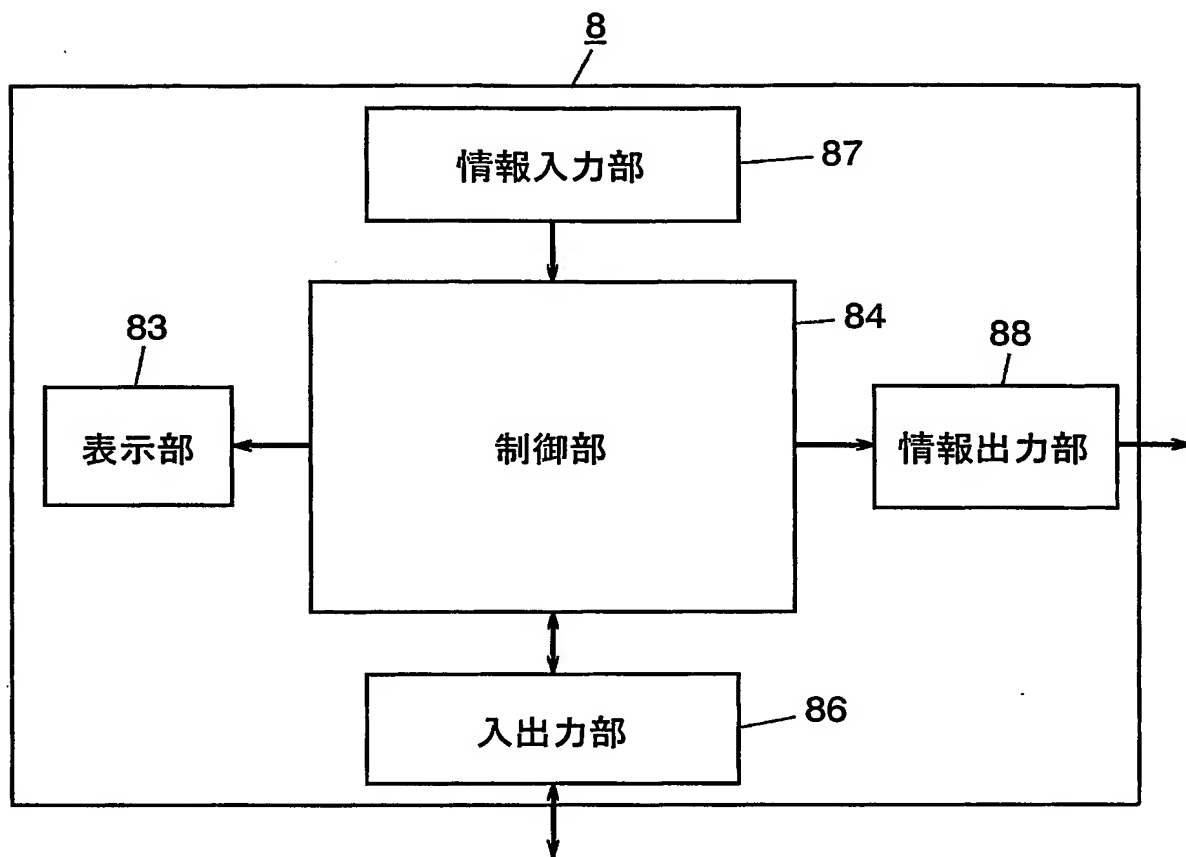
ID 番号	氏名	住所	電話番号	システム 利用	有効期限	登録認証情報	信用情報
1234-5678- 90123-456	松下 太郎	〇〇市××町 1-2-3	045-123-4567	未許可	2004/3/10	Iris00000001	OK

6/15

FIG. 6



7/15
FIG. 7



8/15

FIG. 8

申請時

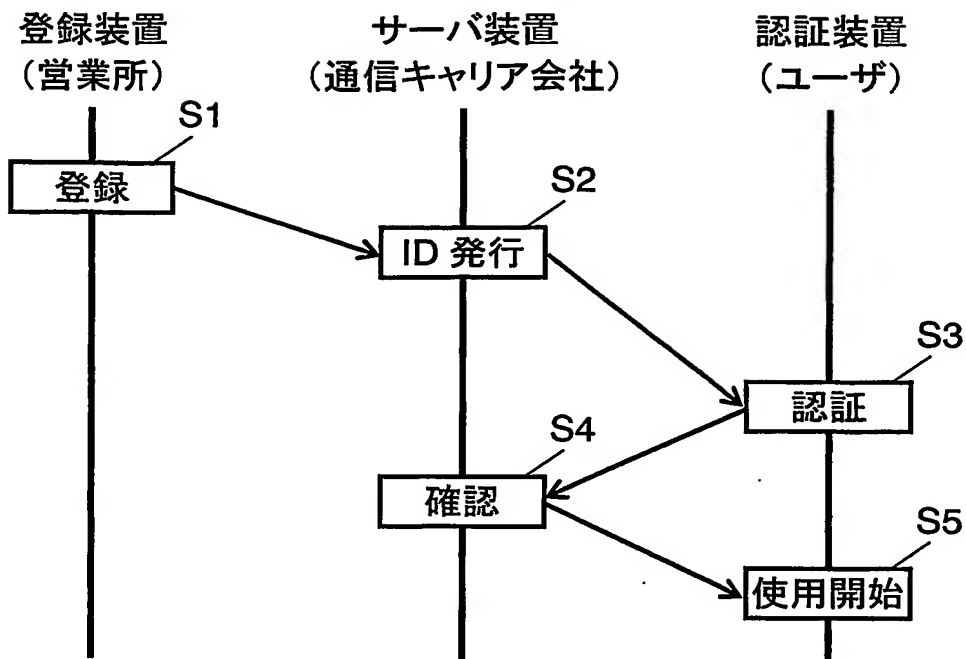
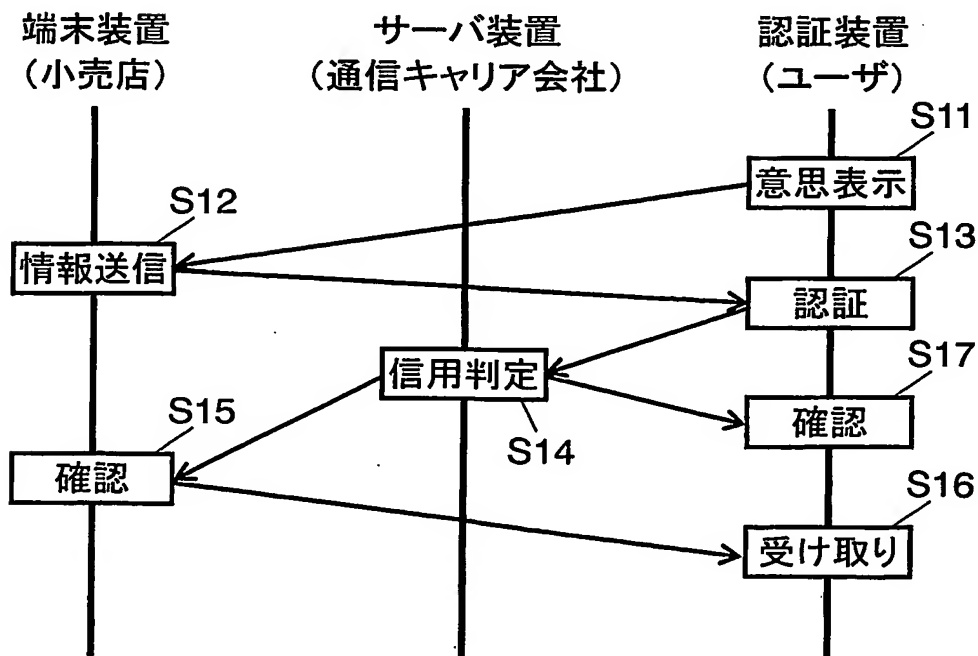


FIG. 9


物品の購買時



9/15

FIG. 10

11

MOBILE CREDIT 利用申請			
利用申請データ作成完了しました。 申請する場合は申請ボタンを押して下さい。			
お名前	TARO MATSUSHITA	生年月日	1978 年 3 月 28 日
住所	〇〇市××町 1-2-3		
電話番号	045-123-4567	携帯電話番号	090-1234-5678
勤務先名	ZZ 株式会社		
勤務先住所	〇〇市△△町 4-5-6		
勤務先電話番号	045-345-6789		
申請日	2003 年 3 月 10 日	有効期限	2004 年 3 月 10 日
<input type="button" value="申請"/>			

10/15

FIG. 11A

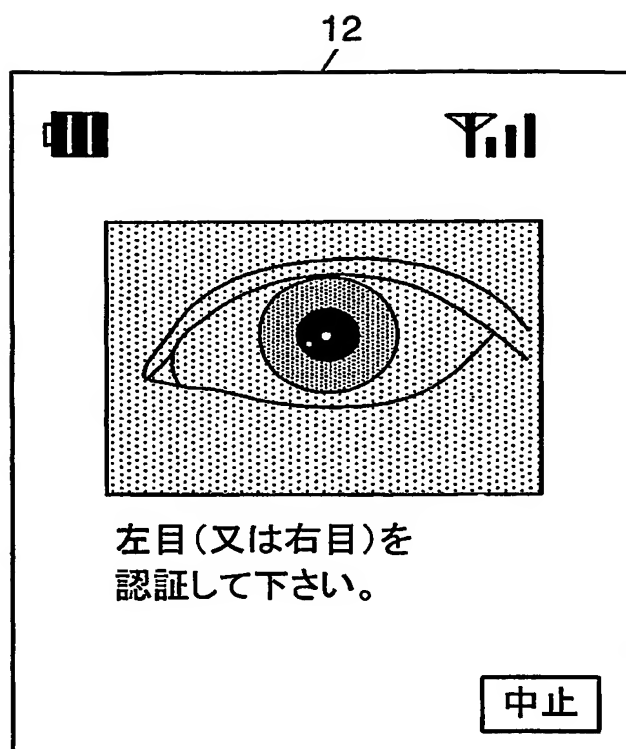
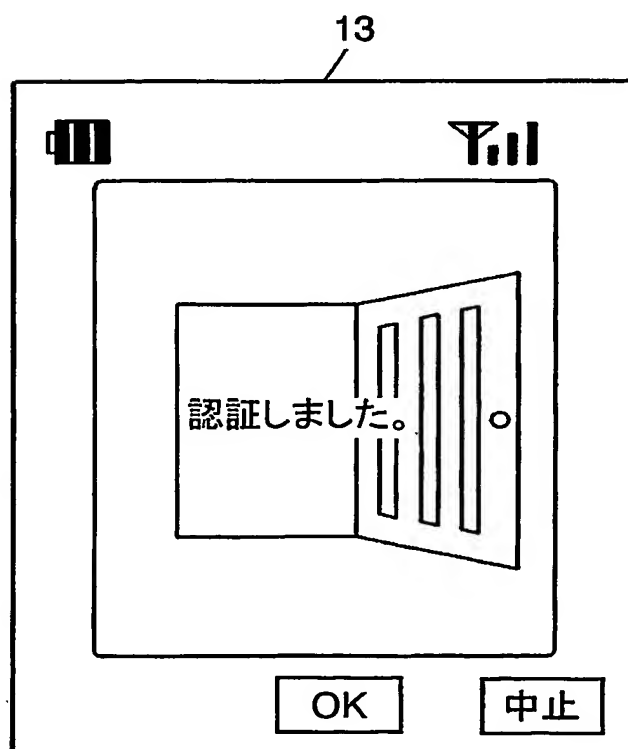


FIG. 11B



11/15

FIG. 12

14

The image shows a mobile phone screen with a credit card interface. At the top, there are two status icons: a signal strength indicator on the left and a battery level indicator on the right. Below these is a rounded rectangular button labeled "MOBILE CREDIT". Underneath this button is a rectangular box containing the text "ID No." followed by the number "1234-5678-90123-456". Below the ID box, there are two more boxes: one on the left containing "Name" and "TARO MATSUSHITA", and one on the right containing a portrait of a man. Below the name box is another box containing "ご利用限度額" (Maximum Usage Limit) and "50,000円". Below the limit box, the text "有効期限" (Valid Period) is followed by "2004年3月10日". At the bottom of the screen, there are four buttons: "サブメニュー" (Sub Menu), a directional pad (four arrows pointing up, down, left, and right), "保存" (Save), and "戻る" (Back).

MOBILE CREDIT

ID No.
1234-5678-90123-456

Name
TARO MATSUSHITA

ご利用限度額
50,000円

有効期限 2004年3月10日

サブメニュー ◀ ▶ ▲ ▼ 保存 戻る

12/15

FIG. 13

商品リスト	
レディースバッグ 商品 No. 05453 19,800 円	ネクタイ 商品 No. 06821 8,000 円
ブーツ 商品 No. 02380 25,000 円	カエルの置物 商品 No. 01478 1,500 円

15

13/15

16

FIG. 14A

クレジット決済	
クレジット利用明細	
下記の内容でよろしければ、決済をします。	
ID No.	1234-5678-90123-456
Name	TARO MATSUSHITA
ご利用年月日	2003年3月14日(金) 19:24
ネクタイ 1本	¥8,000
消費税	¥400
お買上合計	¥8,400
クレジット取引合計	¥8,400
口座番号	0123456789*10
承認番号	0003157216948
決済完了	

17

FIG. 14B

クレジット利用明細	
お客様お控え	
2003年3月14日(金) 19:24	
ネクタイ	
	1本 ¥8,000
消費税	¥400
お買上合計	¥8,400
クレジット取引合計	¥8,400
口座番号	0123456789*10
承認番号	0003157216948
 <input type="button" value="保存"/> <input type="button" value="戻る"/>	

図面の参照符号の一覧表

1	認証システム
2	ユーザ
3	認証装置
4	ネットワーク
5	通信キャリア会社
6	サーバ装置
7	小売店
8	端末装置
9	登録装置
10	営業所
11	申請画面
12	認証開始画面
13	認証完了画面
14	利用許可画面
15	商品リスト画面
16	取引確認画面
17	取引完了画面
31	光学系
33, 93	画像入力部
34	演算部
35	記憶部
36, 66, 86, 96	入出力部
37, 83, 95	表示部
38	光源
39	鏡部
40	切出部
41	コード化部
42	判定部
43	復号化部
50	登録認証情報
51	(金融機関の) サーバ
60	認証処理部
61, 84, 94	制御部
62	データベース部
64	暗号化部

15/15

7 0 登録認証情報テーブル
8 0 金融機関
8 7, 9 7 情報入力部
8 8 情報出力部
9 1 認証情報作成部

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/008854

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F17/60, G06F15/00, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F17/60, G06F15/00, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE(JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2003-186846 A (NTT Data Corp.), 04 July, 2003 (04.07.03), Full text; Figs. 1 to 10 (Family: none)	1-3, 6, 7, 10; 12, 15, 16
Y		4, 5, 8, 9, 11, 13, 14, 17, 18
Y	JP 2002-297551 A (Mitsubishi Electric Corp.), 11 October, 2002 (11.10.02), Full text; Figs. 1 to 9 (Family: none)	8, 11, 13, 14
Y	JP 2002-183638 A (Aruze Kabushiki Kaisha), 28 June, 2002 (28.06.02), Par. Nos. [0049] to [0062]; Figs. 16 to 22 (Family: none)	4, 5, 9, 17, 18

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 July, 2004 (22.07.04)

Date of mailing of the international search report

17 August, 2004 (17.08.04)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/008854

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-297275 A (Future Financial Strategy Kabushiki Kaisha), 26 October, 2001 (26.10.01), Par. Nos. [0045] to [0056]; Fig. 4 (Family: none)	4, 5, 9, 17, 18
A	JP 2003-6549 A (NEC Soft Kabushiki Kaisha), 10 January, 2003 (10.01.03), Full text; Figs. 1 to 2 (Family: none)	1-18
A	JP 2001-266034 A (Casio Computer Co., Ltd.), 28 September, 2001 (28.09.01), Full text; Figs. 1 to 7 (Family: none)	1-18

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. G06F17/60, G06F15/00, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. G06F17/60, G06F15/00, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2004年
 日本国登録実用新案公報 1994-2004年
 日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS), WPI, INSPEC (DIALOG)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2003-186846 A(株式会社エヌ・ティ・ティ・データ) 2003.07.04, 全文, 図1-10 (ファミリーなし)	1-3, 6, 7, 10, 12, 15, 16
Y		4, 5, 8, 9, 11, 13, 14, 17, 18
Y	JP 2002-297551 A(三菱電機株式会社)2002.10.11, 全文, 図1-9 (ファミリーなし)	8, 11, 13, 14
Y	JP 2002-183638 A(アルゼ株式会社)2002.06.28, 【0049】 - 【0062】 段落, 図16-22 (ファミリーなし)	4, 5, 9, 17, 18

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

22.07.2004

国際調査報告の発送日

17.8.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

小太刀 慶明

5 L

2942

電話番号 03-3581-1101 内線 3562

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-297275 A(フューチャーファイナンスストラテジー株式会社)2001. 10. 26, 【0045】 - 【0056】 段落, 図4 (ファミリーなし)	4, 5, 9, 17, 18
A	JP 2003-6549 A(エヌイーシーソフト株式会社)2003. 01. 10, 全文, 図1-2 (ファミリーなし)	1-18
A	JP 2001-266034 A(カシオ計算機株式会社)2001. 09. 28, 全文, 図1-7 (ファミリーなし)	1-18